What is claimed is:

1. A system for securely authenticating a data exchange session with an implantable medical device, comprising:

a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session; and

an external source to establish a secure connection with a secure key repository to securely maintain the crypto key, and to authenticate authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository.

2. A system according to Claim 1, wherein the external source transacts a data exchange session using the crypto key to authenticate the data.

3. A system according to Claim 2, further comprising:

an authentication component to employ the crypto key during the data exchange session, comprising at least one of:

a command authenticator to authenticate commands exchanged through the external source with the implantable medical device and ;

a data integrity checker to check the integrity of the data received by and transmitted from the external source; and

a data encrypter to encrypt the data received by and transmitted from the external source.

4. A system according to Claim 1, further comprising:

a short range interface logically defining a secured area around the implantable medical device in which to establish the secure connection; and

a long range interface logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session.

5. A system according to Claim 1, further comprising:

a key generator to statically generate the crypto key, and to persistently store the crypto key in the secure key repository.

6. A system according to Claim 5, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater.

7. A system according to Claim 5, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

8. A system according to Claim 1, further comprising:

a key generator to dynamically generate the crypto key.

9. A system according to Claim 8, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater.

10. A system according to Claim 8, wherein the crypto key is securely retrieved from the secure key repository through at least one of a programmer and a repeater.

11. A system according to Claim 1, wherein the crypto key is maintained on the implantable medical device, further comprising:

a short range telemetry interface retrieving the crypto key through short range telemetry.

12. A system according to Claim 11, wherein the short range telemetry comprises inductive telemetry.

13. A system according to Claim 11, wherein the external source comprises a programmer.

14. A system according to Claim 13, wherein the crypto key is provided from the programmer to a repeater.

15. A system according to Claim 11, wherein the external source comprises a patient designator.

16. A system according to Claim 15, wherein the crypto key is provided from the patient designator to at least one of a programmer and a repeater.

17. A system according to Claim 1, further comprising:
a secure database to maintain the crypto key; and
a secure server providing the crypto key through a secure connection.

18. A system according to Claim 17, wherein the secure connection comprises at least one of a serial or hardwired connection and a secure network connection.

19. A system according to Claim 17, wherein the external source comprises a programmer.

20. A system according to Claim 19, wherein the crypto key is provided from the programmer to a repeater.

21. A system according to Claim 1, further comprising:
a physical token to maintain the crypto key; and
a reader to retrieve the crypto key by accessing the physical token.

22. A system according to Claim 21, further comprising:
a physical label to specify the crypto key on the physical token.

23. A system according to Claim 22, wherein the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication.

24. A system according to Claim 21, further comprising:
internal storage to specify the crypto key on the physical token.

25. A system according to Claim 24, wherein the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium.

26. A system according to Claim 21, wherein the physical token is accessed using magnetic, optical, serial, and physical reading.

27. A system according to Claim 1, wherein the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key.

28. A system according to Claim 1, wherein the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key.

29. A system according to Claim 1, wherein implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device.

30. A method for securely authenticating a data exchange session with an implantable medical device, comprising:

defining a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session;

establishing a secure connection from an external source with a secure key repository securely maintaining the crypto key; and

authenticating authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository.

31. A method according to Claim 30, further comprising:

transacting a data exchange session through the external source using the crypto key to authenticate the data.

32. A method according to Claim 31, further comprising:

employing the crypto key during the data exchange session, comprising at least one of:

authenticating commands exchanged through the external source with the implantable medical device and ;

checking the integrity of the data received by and transmitted from the external source; and

encrypting the data received by and transmitted from the external source.

33. A method according to Claim 30, further comprising:

logically defining a secured area around the implantable medical device in which to establish the secure connection; and

logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session.

34. A method according to Claim 30, further comprising:

statically generating the crypto key; and

persistently storing the crypto key in the secure key repository.

35. A method according to Claim 34, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater.

36. A method according to Claim 35, further comprising:

securely retrieving the crypto key from the secure key repository through a programmer.

37. A method according to Claim 30, further comprising:

dynamically generating the crypto key.

38. A method according to Claim 37, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater.

39. A method according to Claim 37, further comprising:

securely retrieving the crypto key from the secure key repository through at least one of a programmer and a repeater.

40. A method according to Claim 30, further comprising:

maintaining the crypto key on the implantable medical device; and

retrieving the crypto key through short range telemetry.

41. A method according to Claim 40, wherein the short range telemetry comprises inductive telemetry.

42. A method according to Claim 40, wherein the external source comprises a programmer.

43. A method according to Claim 42, further comprising:

providing the crypto key from the programmer to a repeater.

44. A method according to Claim 40, wherein the external source comprises a patient designator.

45. A method according to Claim 44, further comprising:

providing the crypto key from the patient designator to at least one of a programmer and a repeater.

46. A method according to Claim 30, further comprising:

maintaining the crypto key in a secure database; and

retrieving the crypto key through a secure connection.

47. A method according to Claim 46, wherein the secure connection comprises at least one of a serial or hardwired connection and a secure network connection.

48. A method according to Claim 46, wherein the external source comprises a programmer.

49. A method according to Claim 48, further comprising:
providing the crypto key from the programmer to a repeater.

50. A method according to Claim 30, further comprising:
maintaining the crypto key on a physical token; and
retrieving the crypto key by accessing the physical token.

51. A method according to Claim 50, further comprising:
specifying the crypto key on the physical token using a physical label.

52. A method according to Claim 51, wherein the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication.

53. A method according to Claim 50, further comprising:
specifying the crypto key on the physical token using internal storage.

54. A method according to Claim 53, wherein the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium.

55. A method according to Claim 50, further comprising:
accessing the physical token using magnetic, optical, serial, and physical reading.

56. A method according to Claim 30, wherein the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key.

57. A method according to Claim 30, wherein the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key.

58. A method according to Claim 30, wherein implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device.

59. An apparatus for securely authenticating a data exchange session with an implantable medical device, comprising:

means for defining a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session;

means for establishing a secure connection from an external source with a secure key repository securely maintaining the crypto key; and

means for authenticating authorization to access data on the implantable medical device by means for securely retrieving the crypto key from the secure key repository.

60. A system for securely transacting a data exchange session with an implantable medical device, comprising:

a short range interface to provide communication with an implantable medical device by authenticating access to a securely maintained crypto key;

a long range interface to commence a data exchange session upon successful access authentication with the implantable medical device, and to transact the data exchange session using the crypto key.

61. A system according to Claim 60, wherein the patient health information in maintained in an encrypted form.

62. A system according to Claim 60, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

a short range telemetric connection with the implantable medical device;

a short range telemetric device to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device.

63. A system according to Claim 60, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

a short range telemetric connection with the implantable medical device;

a patient designator to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device.

64. A system according to Claim 60, wherein the authenticating with the implantable medical device is by using a physical token, further comprising:

a physical token; and

a reader to receive the crypto key from the physical token.

65. A system according to Claim 60, wherein the patient health information is maintained in the implantable medical device in unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection.

66. A system according to Claim 65, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

a short range telemetric connection with the implantable medical device;

an external source to send a session crypto key to the implantable medical device; and

an encrypter to encrypt the patient health information maintained in the implantable medical device.

67. A system according to Claim 60, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

a patient designator to establish a short range telemetric connection with the implantable medical device, and to send a session crypto key to the implantable medical device; and

an encrypter to encrypt the patient health information maintained in the implantable medical device.

68. A system according to Claim 60, wherein the long range interface is augmented using one or more repeaters.

69. A method for securely transacting a data exchange session with an implantable medical device, comprising:

providing communication with an implantable medical device by authenticating access to a securely maintained crypto key using a short range interface;

commencing a data exchange session by transitioning to long range interface upon successful access authentication with the implantable medical device; and

transacting the data exchange session using the crypto key.

70. A method according to Claim 69, wherein the patient health information in maintained in an encrypted form.

71. A method according to Claim 69, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

establishing a short range telemetric connection with the implantable medical device;

requesting the crypto key from the implantable medical device; and

receiving the crypto key from the implantable medical device.

72. A method according to Claim 69, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

establishing a short range telemetric connection between the implantable medical device and the patient designator;

requesting for the crypto key from the implantable medical device; and

receiving the crypto key from the implantable medical device.

73. A method according to Claim 69, wherein the authenticating with the implantable medical device is by using a physical token, further comprising:

accessing the physical token; and

receiving the crypto key from the physical token.

74. A method according to Claim 69, wherein the patient health information is maintained in the implantable medical device in unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection.

75. A method according to Claim 74, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

establishing a short range telemetric connection with the implantable medical device;

sending a session crypto key to the implantable medical device; and

encrypting the patient health information maintained in the implantable medical device.

76. A method according to Claim 69, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

establishing a short range telemetric connection with the implantable medical device through the patient designator;

sending a session crypto key to the implantable medical device; and

encrypting the patient health information maintained in the implantable medical device.

77. A method according to Claim 69, wherein the long range interface is augmented using one or more repeaters.

78. An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

means for providing communication with an implantable medical device by means for authenticating access to a securely maintained crypto key using a short range interface;

means for commencing a data exchange session by means for transitioning to long range interface upon successful access authentication with the implantable medical device; and

means for transacting the data exchange session by accessing patient health information stored on the implantable medical device using the crypto key.

79. A system for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

a secure server to provide identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key;

a secure external source to request the crypto key via a secure connection based on the identification of and authentication to access the implantable medical device, and to receive the crypto key; and

a long range interface to commence a data exchange session upon successful access authentication with the implantable medical device, and to transact the data exchange session using the crypto key.

80. A method for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

providing identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key;

requesting the crypto key via a secure connection based on the identification of and authentication to access the implantable medical device; and

receiving the crypto key;

commencing a data exchange session by transitioning to long range interface upon successful access authentication with the implantable medical device; and

transacting the data exchange session using the crypto key.

81. An apparatus for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

means for providing identification of and authentication to access an implantable medical device by means for authenticating access to a securely maintained crypto key;

means for requesting the crypto key via a secure connection based on the identification of and authentication to access the implantable medical device; and

means for receiving the crypto key;

means for commencing a data exchange session by means for transitioning to long range interface upon successful access authentication with the implantable medical device; and

means for transacting the data exchange session using the crypto key.